BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

Attorney Docket # 5284-28 Patent

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Henri GILBERT et al.

Serial No.: 10/736,752

Filed: December 16, 2003

For: A Method of Encipherment by Permutations of Fixed-Length Sequences

Mail Stop
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

LETTER TRANSMITTING PRIORITY DOCUMENT

SIR:

In order to complete the claim to priority in the above-identified application under 35 U.S.C. §119, enclosed herewith is a certified copy of the foreign application on which the claim of priority is based: Application No. **02/15985,** filed on December 17, 2002, in France.

Respectfully submitted,
COHEN, PONTANI, LIEBERMAN & PAVANE

By _____
Thomas Langer
Reg. No. 27,264
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: 5 April 2004

R E P U B L I Q U E F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

10/736,752

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 10 NOV. 2003

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

17 DEC 2002
75 INPI PARIS

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*01

REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 W /260899

Réservé à l'INPI

REMISE DES PIÈCES 0215985
DATE
LIEU
N° D'ENREGISTREMENT
NATIONAL ATTRIBUÉ PAR L'INPI
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 17 DEC. 2002

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

Monsieur Didier LEMOYNE
FRANCE TELECOM R&D/VAT/PI
38-40, rue du Général Leclerc

92794 ISSY MOULINEAUX Cédex 9

Vos références pour ce dossier *(facultatif)* 04411

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE	Cochez l'une des 4 cases suivantes
Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date / /
ou demande de certificat d'utilité initiale	N° Date / /
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date / /

3 **TITRE DE L'INVENTION** (200 caractères ou espaces maximum)

PROCEDE DE CHIFFREMENT PAR PERMUTATIONS DE SUITES DE LONGUEUR FIXEE

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE	
	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

5 DEMANDEUR		☐ **S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»**
Nom ou dénomination sociale		FRANCE TELECOM
Prénoms		
Forme juridique		Société anonyme
N° SIREN		3 8 0 1 2 9 8 6 6
Code APE-NAF		
Adresse	Rue	6, place d'Alleray
	Code postal et ville	75015 PARIS
Pays		France
Nationalité		Française
N° de téléphone *(facultatif)*		
N° de télécopie *(facultatif)*		
Adresse électronique *(facultatif)*		

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE 2/2

REMISE DES PIÈCES DATE	17 DEC 2002 à l'INPI 75 INPI PARIS
LIEU	
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI	0215985

DB 540 W /260899

Vos références pour ce dossier : *(facultatif)*		04411
6 MANDATAIRE		
Nom		LEMOYNE
Prénom		Didier
Cabinet ou Société		FRANCE TELECOM R&D/VAT/PI
N °de pouvoir permanent et/ou de lien contractuel		PG 8300
Adresse	Rue	38-40, rue du Général Leclerc
	Code postal et ville	92794 ISSY MOULINEAUX Cédex 9
N° de téléphone *(facultatif)*		01 45 29 45 24
N° de télécopie *(facultatif)*		01 45 29 65 60
Adresse électronique *(facultatif)*		didier.lemoyne@francetelecom.com
7 INVENTEUR (S)		
Les inventeurs sont les demandeurs		☐ Oui ☒ Non **Dans ce cas fournir une désignation d'inventeur(s) séparée**
8 RAPPORT DE RECHERCHE		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance		**Paiement en deux versements, uniquement pour les personnes physiques** ☐ Oui ☐ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Requise antérieurement à ce dépôt *(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence)* :
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)

Didier LEMOYNE
Mandataire par pouvoir PG 8300

VISA DE LA PRÉFECTURE OU DE L'INPI

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

PROCEDE DE CHIFFREMENT PAR PERMUTATIONS DE SUITES DE LONGUEUR FIXEE

La présente invention concerne un procédé de chiffrement d'une information constituée par une suite finie de N symboles choisis dans un alphabet.

La présente invention se situe dans le domaine technique général du traitement de l'information, et, plus particulièrement, dans celui du chiffrement de l'information par cryptographie à clé secrète symétrique, par opposition à la cryptographie publique à clé asymétrique.

Il arrive fréquemment que l'on ait besoin de chiffrer une information alors que celle-ci est constituée d'une suite finie de symboles appartenant à un alphabet fini, et que l'on souhaite que l'information chiffrée soit elle-même représentée dans ce même alphabet et soit de même longueur que la suite claire initiale. Ce besoin se fait sentir, par exemple, à propos d'un numéro de téléphone, d'un numéro de carte prépayée virtuelle, d'un numéro de carte bancaire, ou encore d'un numéro de licence alphanumérique. Dans les trois premiers cas cités, l'alphabet est constitué de chiffres de 0 à 9, tandis que dans le dernier cas il est constitué de lettres majuscules et minuscules et de chiffres.

C'est un objet de la présente invention que de proposer un procédé de chiffrement basé sur la construction de fonctions de chiffrement que l'on peut désigner par « permutations sur l'ensemble des suites de longueur fixée sur un ensemble fini de symboles », et qui répondrait au besoin exprimer plus haut, quel que soit l'ensemble fini de symboles et quelle que soit la longueur fixée des suites.

La cryptographie à clé secrète consiste en la conception et l'étude des fonctions à convention secrète qui permettent à deux parties partageant la connaissance de cette convention secrète d'effectuer les deux opérations appelées « chiffrement » et « déchiffrement » consistant :

- pour le chiffrement, à transformer des données D en des données C,

- pour le déchiffrement, à transformer les données C ci-dessus en les données D,

avec les propriétés suivantes :

- les données C ne peuvent être transformées en les données D que par le truchement de la connaissance de la convention secrète,
- la connaissance de C et D, ou d'un grand nombre de couples {C, D}, ne permet pas de retrouver la convention secrète.

Il existe de nombreux algorithmes de chiffrement à clé secrète connus dont beaucoup sont standardisés, tels que DES, 3DES, AES, IDEA, BLOWFISH, RC2, RC4, etc.

La majorité de ces algorithmes sont utilisés pour chiffrer des suites binaires, indépendamment de la sémantique de ces bits, et nécessitent donc la transformation des informations à chiffrer en un codage binaire. L'information chiffrée résultante est également représentée par une suite binaire.

Il existe plusieurs modes de chiffrement, qui contraignent dans la plupart des cas à chiffrer des blocs binaires de taille fixe. Les différences entre les modes jouent sur les propriétés de synchronisation entre un bloc en clair et un bloc chiffré, par exemple : réinjection d'un bloc chiffré pour le chiffrement du bloc suivant, dictionnaire de blocs chiffrés indépendamment, etc.

Cependant, ces techniques de chiffrement connus présentent un certain nombre d'inconvénients :

a) Dans le cas où l'on veut chiffrer des données indépendantes, de petite taille, les outils existants mènent à une expansion de l'information, soit pour respecter le format de représentation de l'information chiffrée, soit pour disposer de clés de diversification (vecteurs d'initialisation) propres à la garantie de sécurité du chiffrement. C'est ainsi, par exemple, que le chiffrement d'un texte constitué de caractères imprimables donne une suite binaire (caractères ASCII notamment) et nécessite une expansion pour pouvoir représenter le texte chiffré sous forme de caractères imprimables.

b) La contrainte de respect du format de l'information à chiffrer comme du format de l'information chiffrée entraîne, dans les outils existants, la perte du format des données claires lors du chiffrement. C'est le cas en particulier du chiffrement d'identifiants numériques, qui généralement sont représentables par

un numéro de série plus petit qu'une valeur maximale, et qui mène à un résultat chiffré n'ayant plus cette propriété.

Aussi, le problème technique à résoudre par l'objet de la présente invention est de proposer un procédé de chiffrement d'une information constituée par une suite finie $\{S_1,S_2,\ldots,S_N\}$ de N symboles choisis dans un alphabet A, qui permettrait de chiffrer une suite de longueur fixée tout en évitant les inconvénients de l'art antérieur mentionnés plus haut.

La solution au problème technique posé consiste, selon la présente invention, en ce que, ayant défini, d'une part, une convention secrète de p symboles de clé $K_1,\ldots,K_p$ choisis dans un deuxième alphabet B et, d'autre part, une fonction multivariée M à m+1 variables (m<=N) : $M(X_{i1},\ldots,X_{im},Y)$ opérant de A^mxB dans A, $\{i_1,\ldots,i_m\}$ étant m indices distincts de l'intervalle [1,N] et la fonction M étant bijective par rapport à au moins une des m variables de A, ledit procédé de chiffrement consiste à effectuer une succession de X permutations sur les suites $\{S_1,S_2,\ldots,S_N\}$ de sorte que, $\{S_1,S_2,\ldots,S_N\}$ étant la suite avant la $j^{ème}$ permutation, la suite après la $j^{ème}$ permutation est $\{S_2,S_3,\ldots, S_N,Zj\}$, Zj étant égal à $M(S_{i1},\ldots,S_{im},K_j)$, l'information chiffrée étant constituée par la suite $\{S'_1,S'_2,\ldots,S'_N\}$ obtenue à l'issue de la $X^{ème}$ permutation.

Dans la suite de ce mémoire on appellera « symbole » une unité élémentaire d'information qui sert à représenter des mots, des nombres, des noms, etc. Des exemples de symboles sont le bit, l'octet, les caractères imprimables, les chiffres, etc.

De même, on désignera par « alphabet » un ensemble de symboles ayant une propriété commune, par exemple sur le format, la taille, etc., qui servent ensemble à représenter une certaine catégorie d'information. On peut citer comme alphabet les caractères sur 7 bits définis par le code ASCII, les chiffres de 0 à 9, les caractères affichables.

Par fonction « multivariée », on entendra une fonction qui prend plusieurs arguments en entrée, ces arguments pouvant être de même nature ou de nature différente. L'addition est un exemple de fonction multivariée. Dans le cadre de l'invention, la fonction multivariée M prend en entrée m symboles $S_{i1},\ldots,S_{im}$ et une valeur K_j de symbole de clé de la convention secrète K, et donnant en sortie un symbole Zj appartenant au même alphabet A que les symboles S_i : $Zj=M(S_{i1},\ldots,S_{im},K_j)$

La fonction multivariée M est dite bijective par rapport à l'une de ses variables si, toutes les autres variables étant fixées, la fonction restreinte à cette coordonnée est bijective. Dans la suite de la description, on considèrera le cas où la fonction $M(X_{i1},...,X_{im},Y)$ est bijective par rapport à la première variable (X_{i1}).

Selon un mode de mise en œuvre particulier du procédé conforme à l'invention dans lequel le nombre m est égal à 3, la fonction M définie par $Z=M(X_1,X_2,X_N,Y)$ se calcule selon les étapes suivantes:

- $U=t1(X_1,X_N)$
- $V=t2(U,Y)$
- $Z=t1(V,X_2)$

t1 et t2 étant les fonctions associées à deux carrés latins T1 et T2 de taille égale au cardinal de l'ensemble A.

On appelle "carré latin" de taille N un tableau T de NxN cases contenant N symboles distincts (S1,...,SN) d'un alphabet A et tel que chaque ligne et chaque colonne du tableau contienne une et une seule fois chaque symbole. Un exemple de carré latin de taille 4 est donné sur la figure 5.

Par extension, et en supposant que les symboles de l'alphabet A soient ordonnés, c'est à dire numérotés de 1 à N, on définit une fonction "carré latin" t, associée au carré latin T, de la manière suivante: t(Si,Sj) est le symbole contenu dans la case située à l'intersection de la $i^{ème}$ ligne et de la $j^{ème}$ colonne.

La fonction multivariée t ainsi définie est bijective par rapport à chacune de ses variables.

On peut définir l'"inverse à gauche" T^{*g} et l'"inverse à droite" T^{*d} d'un carré latin et les fonctions t^{*g} et t^{*d} associées correspondantes par les propriétés :

- quels que soient Y et X, $t(t^{*g}(X,Y),Y)=X$
- quels que soient Y et X, $t(X, t^{*d}(X,Y))=Y$

La description qui va suivre en regard des dessins annexés, donnés à titre d'exemples non limitatifs, fera bien comprendre en quoi consiste l'invention et comment elle peut être réalisée.

La figure 1 est un schéma montrant le mécanisme d'un registre à décalage.

La figure 2 est un schéma montrant le mécanisme d'un premier mode de réalisation du procédé conforme à l'invention.

La figure 3 est un schéma montrant le mécanisme d'un deuxième mode de réalisation du procédé conforme à l'invention.

La figure 4 est un schéma montrant le mécanisme de déchiffrement associé au mécanisme de chiffrement de la figure 3.

La figure 5 représente un exemple de carré latin de taille 4.

Sur la figure 1 est représenté un registre à décalage de longueur N composé d'un ensemble ordonné de N cases contenant N symboles, distincts ou non, d'un alphabet A, à savoir $S_1,S_2,\ldots,S_N$.

Le registre de la figure 1 possède un mécanisme dit de décalage qui, à partir d'un nouveau symbole, mémorise celui-ci dans la dernière case et mémorise dans chaque case j-1 le symbole préalablement présent dans la case j. Par conséquent, le symbole S_1 préalablement présent dans la première case est oublié.

Dans le cadre de l'invention, les N symboles constituant l'information à chiffrer sont disposés initialement dans les N cases du registre à décalage de la figure 1.

Selon le procédé, objet de l'invention, on définit, d'une part, une convention secrète K consistant en une suite de p symboles de clé $K_1, \ldots,K_p$ choisis dans un deuxième alphabet B avec, de préférence, p suffisamment grand, et, d'autre part, une fonction multivariée M à m+1 variables ($m<=N$) : $M(X_{i1},\ldots,X_{im},Y)$ opérant de $A^m xB$ dans A, $\{i_1,\ldots,i_m\}$ étant m indices distincts de l'intervalle [1,N].

Par ailleurs, la fonction M est prise bijective par rapport à sa première variable X_{i1}.

Dans un mode général de mise en œuvre du procédé de chiffrement, objet de l'invention, représenté sur la figure 2, le nombre m est égal à N: $(\{i_1,\ldots,i_m\}=\{1,\ldots,N\})$.

Soit alors $Zj=M(S_1,\ldots,S_N,K_j)$ le résultat du $J^{ème}$ tour du registre à décalage. Si $\{S_1,S_2, \ldots,S_N\}$ est l'état du registre à décalage avant le $J^{ème}$ tour, l'état du registre à décalage après le $J^{ème}$ tour et avant le $J+1^{ème}$ tour devient : $\{S_2,S_3,\ldots,S_N,Z_j\}$.

Le procédé de chiffrement consiste à effectuer X tours du registre à décalage, avec X de préférence supérieur à plusieurs fois N. L'état du registre à

décalage avant le 1er tour constitue l'information en clair. L'état du registre à décalage à l'issue du X^{ème} tour constitue l'information chiffrée.

Dans une variante du procédé de l'invention, le nombre m est pris strictement inférieur à N, par exemple 3, et la fonction M est définie par $M(X_1,X_2,X_N,Y)$, comme indiqué sur la figure 3: $\{i_1,i_2,i_3\}=\{1,2,N\}$. Le résultat Zj du J^{ème} tour du registre à décalage est donné par $Zj= M(S_1,S_2,S_N,K_j)$.

Une mise en œuvre particulière de cette variante de réalisation consiste par exemple à choisir pour alphabet A l'ensemble des chiffres de 0 à 9.

La longueur N des suites $\{S_1,S_2, \ldots,S_N\}$ peut prendre des valeurs différentes de 6 à 16 environ, par exemple N=14. Toute autre valeur serait évidemment recevable.

Le registre à décalage est donc de taille N=14.

La convention secrète K est constituée d'une suite de p=12 chiffres, par exemple: K1,...,K12. Si le nombre X de tours de registre à décalage est supérieur à p, on prendra K13=K1, K14=K2, etc.

On appellera T1 et T2 deux carrés latins de taille N=10 sur l'alphabet A, et t1 et t2 les fonctions associées.

La fonction M prend en argument trois cases du registre à décalage : la première X1, la deuxième X2 et la dernière X14. $Zj=M(S_1,S_2,S_N,K_j)$ est calculé avec un symbole de clé K_j choisi dans la convention secrète K.

M(X1,X2,X14,Y)=Z se calcule par étapes :

- U=t1(X1,X14)
- V=t2(U,Y)
- Z=t1(V,X2)

Après X=100 tours du registre à décalage, par exemple, on obtient l'information initiale chiffrée que l'on notera sous forme de la suite $\{S'_1,S'_2, \ldots,S'_N\}$.

Conformément à la figure 4, la fonction de déchiffrement de l'information chiffrée $\{S'_1,S'_2, \ldots,S'_N\}$ est construite de la manière suivante :

- En entrée, le registre à décalage est chargé avec les données chiffrées inversées symbole par symbole $(S'_N,S'_{N-1}, \ldots, S'_1)$.
- La fonction inverse « M^{-1} » de M par rapport à la première coordonnée prend en argument trois cases du registre à décalage : la première X1, la deuxième X2 et la dernière X14.

$Zj=M(S_1,S_2,S_N,K_j)$ est calculé avec un symbole de clé Kj, en commençant par le dernier utilisé lors du chiffrement et ensuite en décroissant : au tour suivant est utilisé Kj-1.

- M(X1,X2, X14,Y)=Z se calcule par étapes :
  - $V=t1^{*g}(X1,X14)$
  - $U=t2^{*g}(V,Y)$
  - $Z=t1^{*g}(U,X2)$
- Le registre se décale alors de la même manière que pour la fonction de chiffrement, la $14^{ème}$ case prenant la valeur Zj.
- On effectue ainsi 100 tours du registre à décalage.
- A l'issue de ces 100 tours, le registre contient l'information en clair $\{S_1,S_2, \ldots,S_N\}$.

On comprend que l'avantage de ce procédé est que la fonction de chiffrement et la fonction de déchiffrement ont le même schéma.

REVENDICATIONS

1. Procédé de chiffrement d'une information constituée par une suite finie $\{S_1,S_2,\ldots,S_N\}$ de N symboles $(S_1,S_2,\ldots,S_N)$ choisis dans un alphabet A, caractérisé en ce que, ayant défini, d'une part, une convention secrète (K) de p symboles de clé $K_1,\ldots,K_p$ choisis dans un deuxième alphabet B et, d'autre part, une fonction multivariée M à m+1 variables (m<=N) : $M(X_{i1},\ldots,X_{im},Y)$ opérant de A^mxB dans A, $\{i_1,\ldots,i_m\}$ étant m indices distincts de l'intervalle [1,N] et la fonction M étant bijective par rapport à au moins une (X_{i1}) des m variables de A, ledit procédé de chiffrement consiste à effectuer une succession de X permutations sur les suites $\{S_1,S_2,\ldots,S_N\}$ de sorte que, $\{S_1,S_2,\ldots,S_N\}$ étant la suite avant la $j^{ème}$ permutation, la suite après la $j^{ème}$ permutation est $\{S_2,S_3,\ldots, S_N,Zj\}$, Zj étant égal à $M(S_{i1},\ldots,S_{im},K_j)$, l'information chiffrée étant constituée par la suite $\{S'_1,S'_2,\ldots,S'_N\}$ obtenue à l'issue de la $X^{ème}$ permutation.
2. Procédé de chiffrement selon la revendication 1, caractérisé en ce que la fonction $M(X_{i1},\ldots,X_{im},Y)$ est bijective par rapport à la première variable (X_{i1}).
3. Procédé de chiffrement selon l'une des revendications 1 ou 2, caractérisé en ce que le nombre m est égal à N.
4. Procédé de chiffrement selon l'une des revendications 1 ou 2, caractérisé en ce que le nombre m est strictement inférieur à N.
5. Procédé de chiffrement selon l'une quelconque des revendications 1 à 4, caractérisé en ce que le nombre X de permutations est supérieur à plusieurs fois la longueur N des suites $\{S_1,S_2,\ldots,S_N\}$.
6. Procédé de chiffrement selon la revendication 5, caractérisé en ce que le nombre m est égal à 3, la fonction M étant définie par $M(X_1,X_2,X_N,Y)$.
7. Procédé de chiffrement selon la revendication 6, caractérisé en ce que la fonction $M(X_1,X_2,X_N,Y)=Z$ se calcule selon les étapes suivantes:
   - $U=t1(X_1,X_N)$
   - $V=t2(U,Y)$
   - $Z=t1(V,X_2)$

t1 et t2 étant les fonctions associées à deux carrés latins T1 et T2 de taille égale au nombre N.

8. Procédé de déchiffrement d'une information chiffrée au moyen du procédé de chiffrement selon la revendication 7, caractérisé en ce que les symboles $(S'_1,S'_2,\ldots,S'_N)$ de la suite $\{S'_1,S'_2,\ldots,S'_N\}$ constituant l'information chiffrée étant inversés symbole par symbole $(S'_N,S'_{N-1}, \ldots, S'_1)$, $M(S_1,S_2,S_N,K_j)=Zj$ est calculé en utilisant un symbole de clé Kj en commençant par le dernier utilisé lors du chiffrement et en ensuite en ordre décroissant $\ldots Zj,Zj-1,\ldots$, $M(X_1,X_2,X_N,Y)=Z$ se calculant selon les étapes suivantes:

- $V=t1^{*g}(X_1,X_N)$
- $U=t2^{*g}(V,Y)$
- $Z=t1^{*g}(U,X_2)$,

la suite obtenue à l'issue de la $X^{ème}$ permutation reconstituant l'information en clair $\{S_1,S_2, \ldots,S_N\}$.

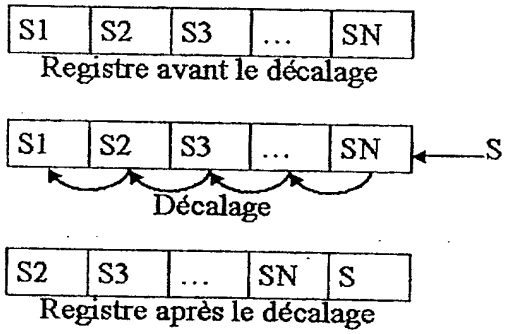

Figure 1

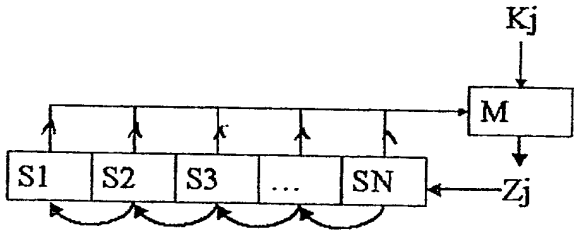

Figure 2

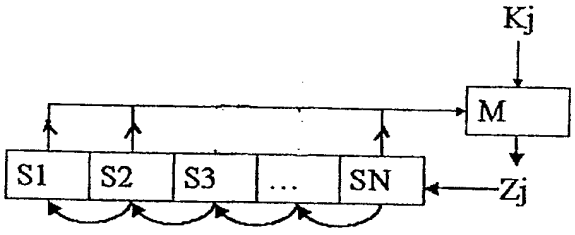

Figure 3

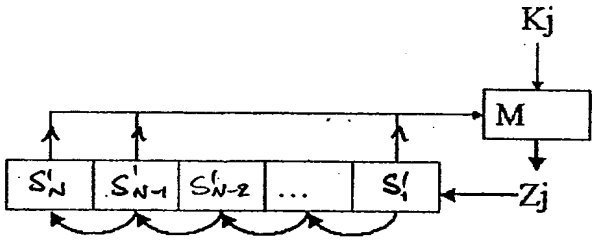

Figure 4

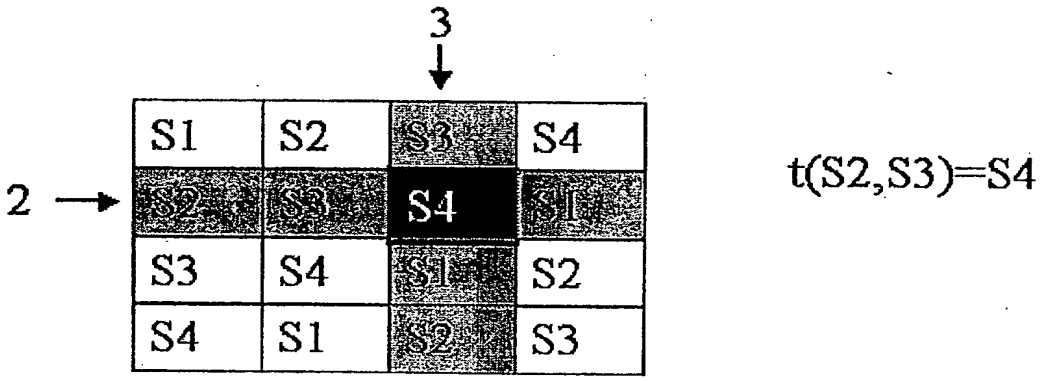

Figure 5

reçue le 20/01/03

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11 235*02

DÉPARTEMENT DES BREVETS
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

DÉSIGNATION D'INVENTEUR(S) Page N° 1 / 1
(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W /260899

Vos références pour ce dossier *(facultatif)*	04411
N° D'ENREGISTREMENT NATIONAL	0215985

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

PROCEDE DE CHIFFREMENT PAR PERMUTATIONS DE SUITES DE LONGUEUR FIXEE

LE(S) DEMANDEUR(S) :

FRANCE TELECOM
6, place d'Alleray
75015 PARIS

DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).

Nom		GILBERT	
Prénoms		Henri	
Adresse	Rue	2, allée des peupliers	
	Code postal et ville	91140	Bures-sur-Yvette
Société d'appartenance *(facultatif)*		France Télécom	
Nom		MACARIO-RAT	
Prénoms		Gilles	
Adresse	Rue	52, rue Jean-Jaurès	
	Code postal et ville	92170	Vanves
Société d'appartenance *(facultatif)*		France Télécom	
Nom		MOUTON	
Prénoms		Dimitri	
Adresse	Rue	11, rue Antoine Bourdelle	
	Code postal et ville	75015	Paris
Société d'appartenance *(facultatif)*		France Télécom	

DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)

10 décembre 2002
Didier LEMOYNE
Mandataire par pouvoir PG 8300